Single Connect Kron

Datasheet

CLOUD-BASED SECURE - ACCESS MANAGEMENT SOLUTIONS

Single Connect is applicable to numerous cloud-based use cases. One of them includes Single Connect as a **Cloud PAM Solution** which enables the management and coordination of secure access to client's distributed infrastructure among on-premise, hybrid and cloud. Another use case positions Single Connect as **PAM as a Service** which supplies multi-tenant secure-access management capability for Cloud providers.

Cloud Privileged Access Management (Cloud PAM)

Single Connect™ protects client organizations' assets whether their infrastructure is on-premise, cloud or hybrid, and supports Cloud IaaS platforms like **Amazon, Azure, Google Cloud and OpenStack**. Single Connect™ Cloud PAM solution secures access, controls configuration changes, records all privileged activities in public and private cloud platforms and supports extremely fast **scale-out** and **scale-in** scenarios by auto discovering and onboarding virtual instances within minutes. All Single Connect™ modules and features are available as a service to use in cloud platforms.

The Challenge

Increase on complexity of an enterprise network infrastructure like hybrid network topology brings increase on overhead of **security risk management** systems for every need of connectivity between one network to another.

The overhead is not about establishing and maintaining technical security check and balance systems but also consuming time and effort for **security leakage**. In order to eliminate the security risks, the main approach is to isolate all networks and do not allow any granting access among networks. However, this hard-protective approach entails business overheads in terms of decision-making processes.

Single Connect Kron

Datasheet

THE SOLUTION-**SINGLE CONNECT™**

CLOUD PAM

As a Cloud PAM solution, Single Connect Cloud™ PAM Solution eliminates the complexity of different network connectivity and mitigates the security risks by centralizing the check and control mechanisms shown in Figure-1.

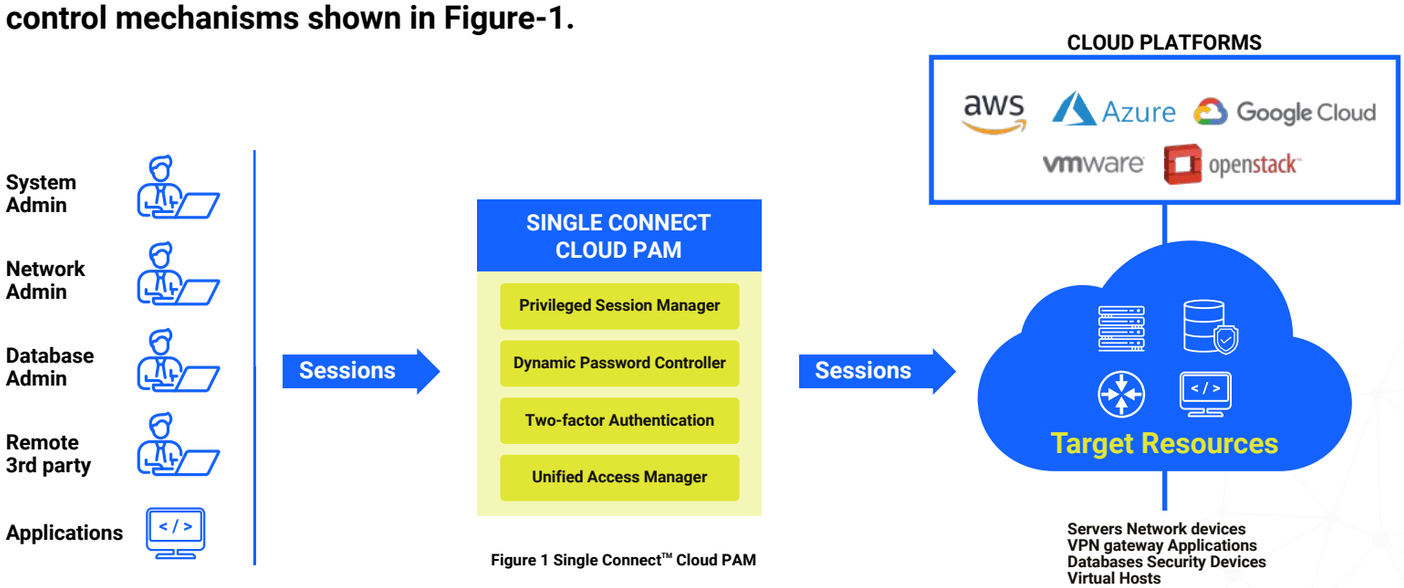
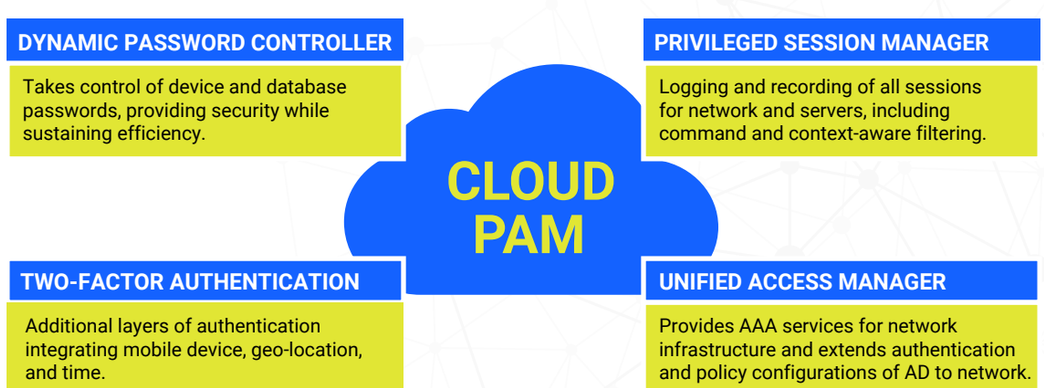


Figure 1 Single Connect™ Cloud PAM

Single Connect™ Cloud PAM Services

Single Connect Cloud™ modules and features are available as a service to use in cloud platforms.



Single Connect Kron

Datasheet

FEATURES & BENEFITS

Single Connect Cloud PAM

Runs **on-premise** and Cloud IaaS platforms including AWS, Azure and Google Cloud.

Tracks and records all **privileged** activities in your Cloud IaaS platform.

Audits trails and reports to meet **regulatory** compliance mandates.

Discovers **system/service** accounts and eliminate password sharing.

Strengthens credentials by eliminating weak or **non-expiry** passwords and SSH keys.

Extends “segregation of duties” to the cloud, manages **who can access** what and when.

Extends “least privilege management” (access under what restrictions) to the cloud with dvanced in-session controls to run a command, including **whitelist/blacklist** filtering, context-aware filtering, geofence approval and managerial approval.

Extends accountability **(who did what)** to cloud IaaS platforms with indisputable log and video records.

Monitors and participates in live sessions, with **take & release** control

Secures and controls **remote** vendor access to your Cloud IaaS Platform.

Single Connect Kron

Datasheet

PRIVILEGED ACCESS MANAGEMENT AS A SERVICE (PAM AS A SERVICE)

The Challenge

As a Cloud provider, by supplying rented or managed VM, OS and other services, there are numerous challenges related with managing **access-security**. If there is no completely isolated network (MPLS) within an enterprise, one of the main challenges is to manage which Cloud provider's **privileged account** will access which VM that functions internally. Moreover, due to **multi-tenant** support needed for a Cloud provider, internal privilege accounts may vary and any breach occurrence needs to be discovered immediately.

Additionally, enterprises that utilize Cloud services, due to their business's regulatory needs, may need to **manage their own internal accounts** activities. In order to accomplish the management of such activities, either they have to integrate their own PAM solution with VMs in the Cloud environment or they have to utilize the **multi-tenant** cloud-based PAM solution provided by the Cloud provider. The first option requires additional costs for the enterprises to cover their regulatory mandatories unless the Cloud provider offers such a service.

The Solution – PAM as a Service

To overcome diverse conflicts that may occur due to internal threats, the unified access **security platform** - Single Connect™ - provides a wide range of protection & monitoring services to Cloud providers in order to manage privileged accounts access to the Cloud infrastructure. Furthermore, **multi-tenant** support of Single Connect™ can be used as a Cloud service for the **Cloud provider's** customers which enables Cloud providers to generate extra revenue stream.

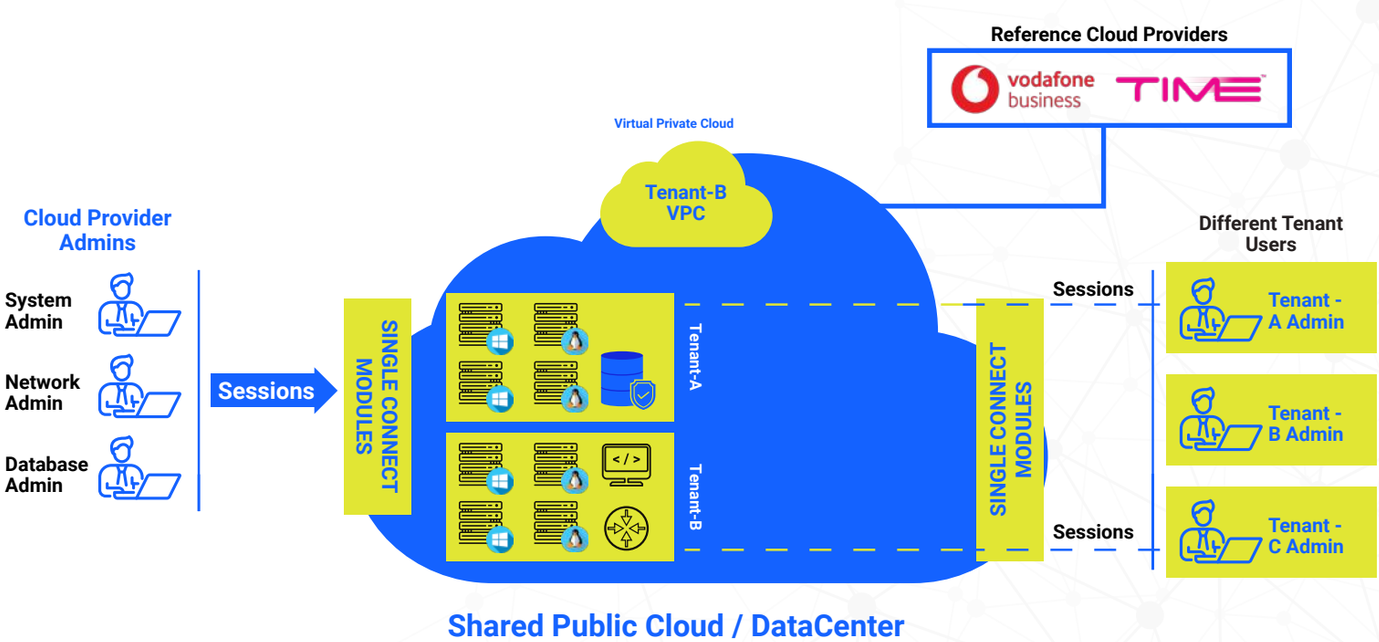


Figure 2 - Cloud Integration Diagram with Single Connect

Single Connect Kron

Datasheet

FEATURES & BENEFITS

Benefits for Cloud Providers	Benefits for Tenants
▸ Mitigates security leakage originated possibly by tenants and keeps it under control without spread.	▸ Tracks and records all privileged activities in Cloud IaaS platform. ▸ Audits trails and reports to meet regulatory compliance mandates. ▸ Discovers system/service accounts and eliminate password sharing.
▸ Lessens the responsibility of cloud servers from security perspective.	▸ Strengthens credentials by eliminating weak or non-expiry passwords and SSH keys. ▸ Extends “segregation of duties” to the cloud, manages who can access what and when.
▸ Enables a cloud service for its customers.	▸ Extends accountability (who did what) on cloud servers regarding to activities with indisputable log and video records.
▸ Generates a new revenue stream.	▸ Monitors and participates in live sessions, with take & release control. ▸ Secures and controls remote vendor access to your Cloud IaaS Platform.